The Multiple Conjugacy Problem

Boaz Tsaban

Partially joint with

David Garber, Arkadius Kalka, Mina Teicher, Gary Vinokur

Bar-Ilan University

GAGTA-6, July/August 2012 CE

Part I

Reductions to the Multiple Conjugacy Problem

Dehn's Problems 1911

$G = \langle X \mid R \rangle$.

Word Problem. Decide whether $g = 1$.

Conjugacy Problem. Decide whether g, h are conjugate.
(AKA Generalized Word Problem.)

Isomorphism Problem. Decide whether G, H are isomorphic.

Originally, decision problems. Crypto uses the search versions.

The Diffie–Hellman KEP

Diffie–Hellman 1976.

Alice	**Public**	**Bob**
$a \in \{0, 1, \ldots, p-1\}$	$G = \langle g \rangle, \ \|G\| = p$	$b \in \{0, 1, \ldots, p-1\}$
	$\boxed{g^a}$ $\longrightarrow$	
	$\longleftarrow$ $\boxed{g^b}$	
$K = \boxed{g^b}^a = g^{ab}$		$K = \boxed{g^a}^b = g^{ab}$

Discrete Logarithm Problem $(g^x \mapsto x) \geq$ Diffie–Hellman KEP.

The Braid Diffie–Hellman KEP

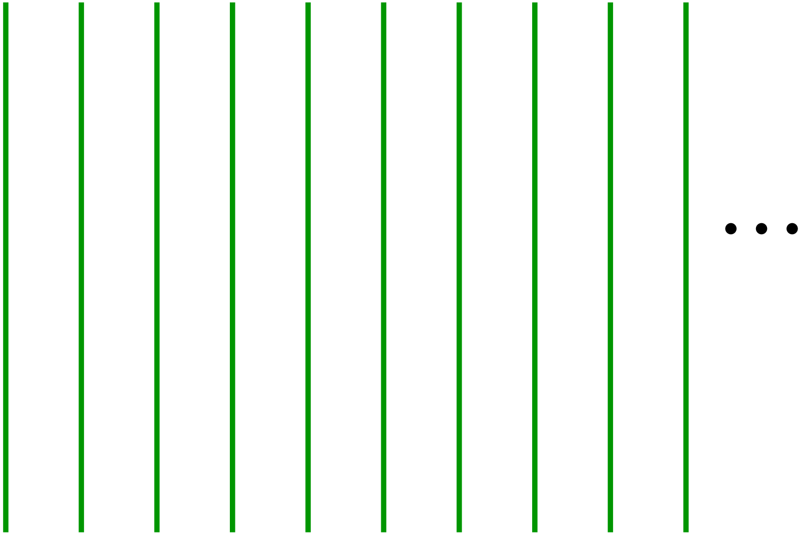
Ko–Lee–Cheon–Han–Kang–Park 2000. G noncommutative.

$g^x := x^{-1} g x$.

Alice	**Public**	**Bob**
$a \in A$	$A, B \leq G, g \in G, [A, B] = 1$	$b \in B$
	$\boxed{g^a}$ $\longrightarrow$	
	$\longleftarrow$ $\boxed{g^b}$	
$K = \boxed{g^b}^a = g^{ba}$		$K = \boxed{g^a}^b = g^{ab}$

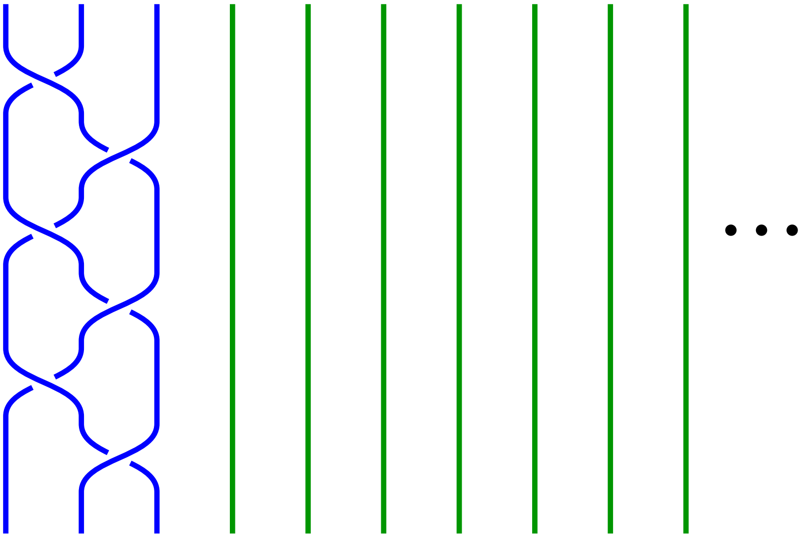
Artin's braid group **B**

Identity braid:



The ordinary braid

$\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2$:



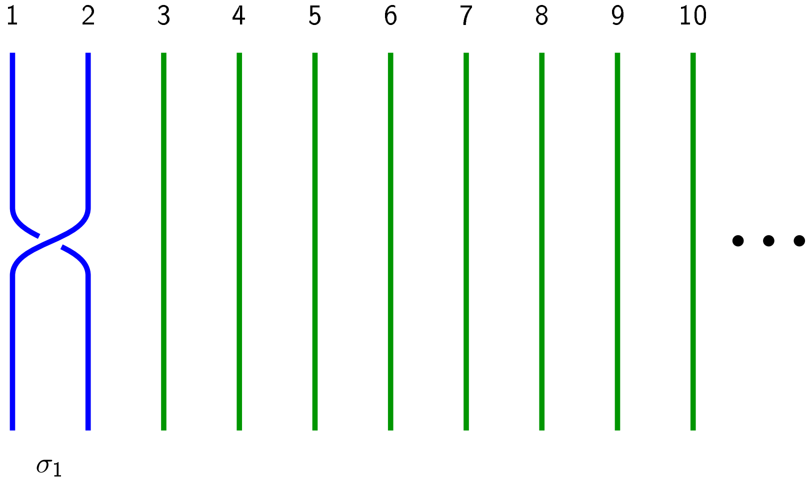
Artin's braid group $\mathbf{B}$

$\mathbf{B}$: Braids / isotopy.

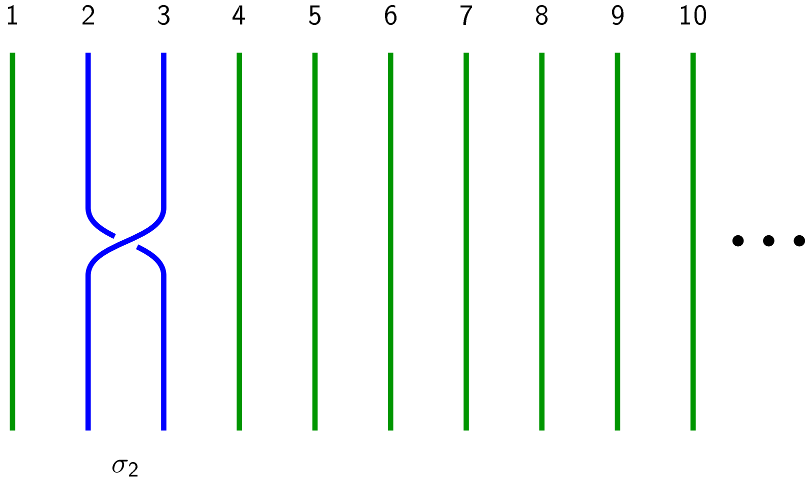
Multiplication: Concatenation of braids.

Inversion: Mirror braid.

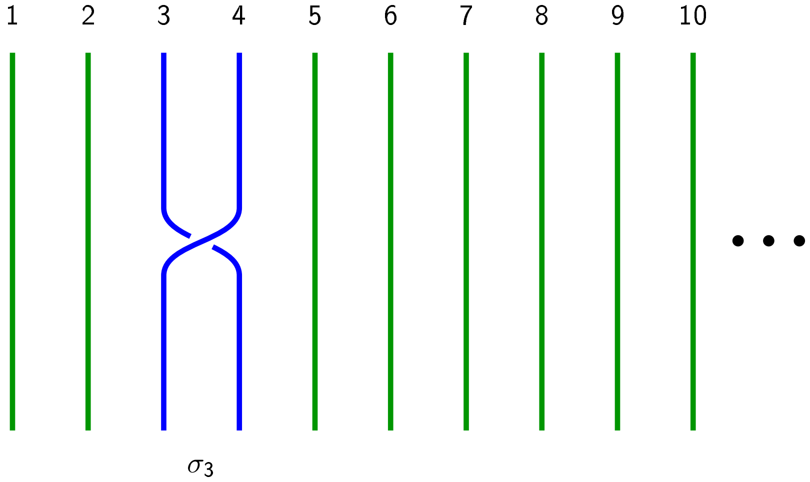
Generators of the braid group



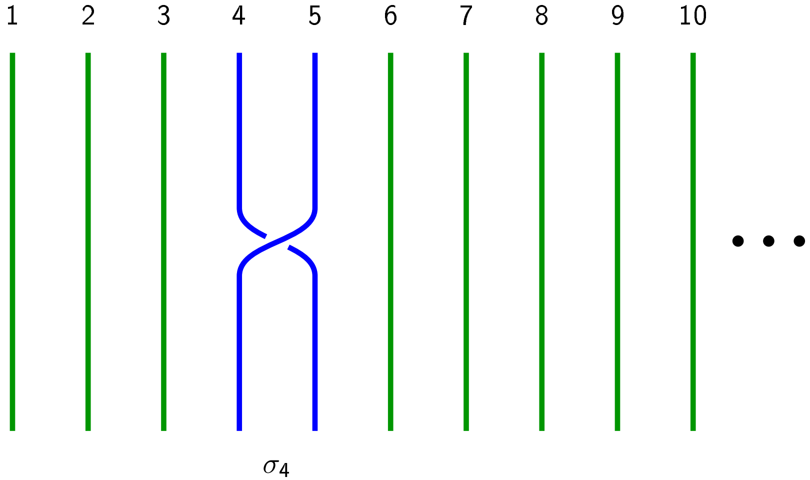
Generators of the braid group



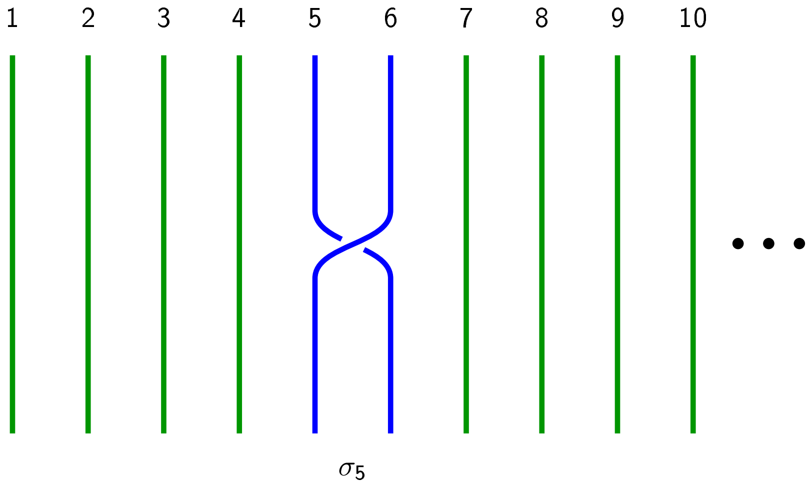
Generators of the braid group



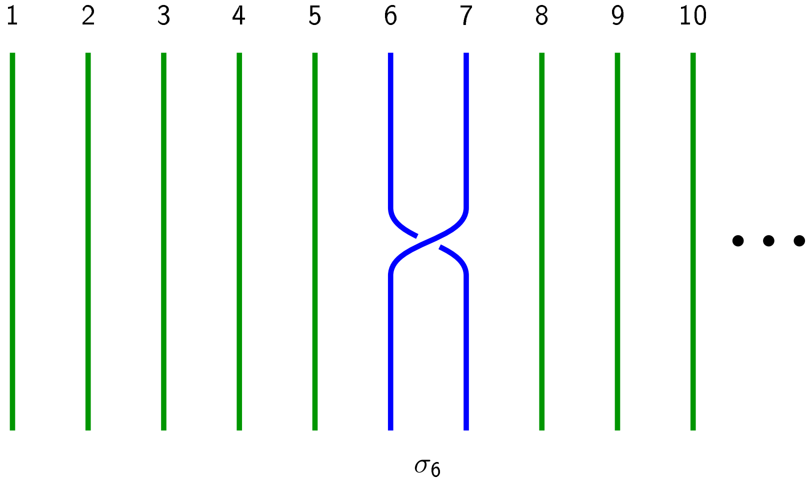
Generators of the braid group



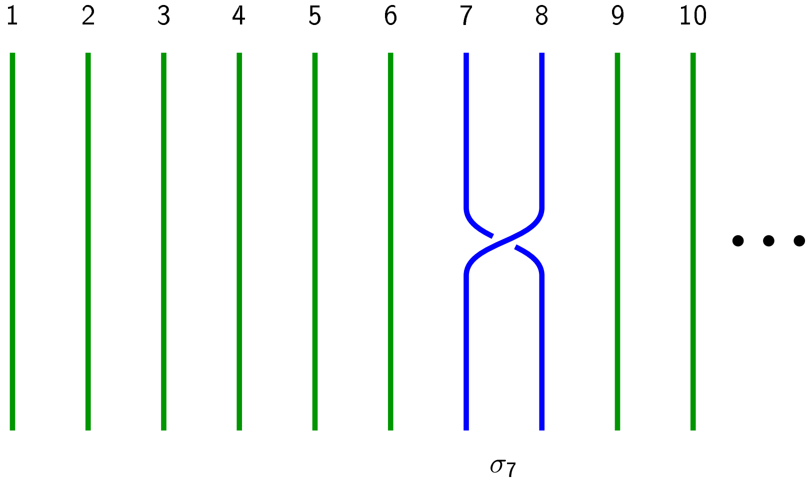
Generators of the braid group



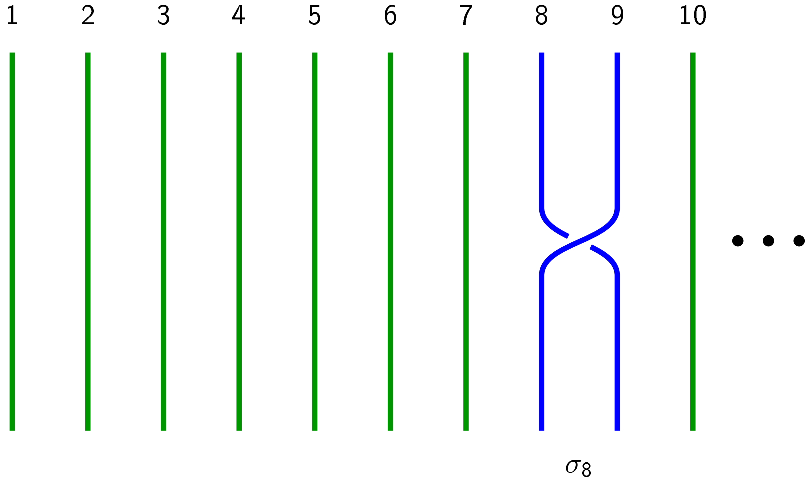
Generators of the braid group



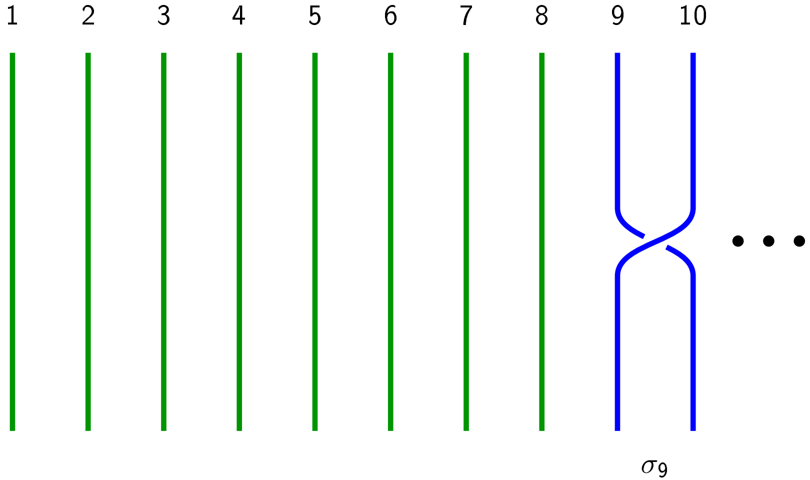
Generators of the braid group



Generators of the braid group

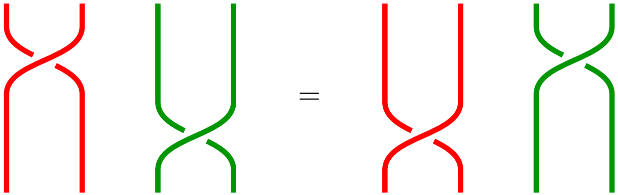


Generators of the braid group

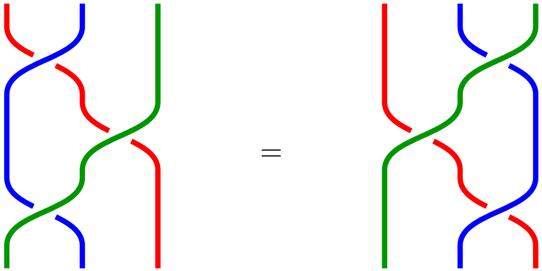


Relations in the braid group

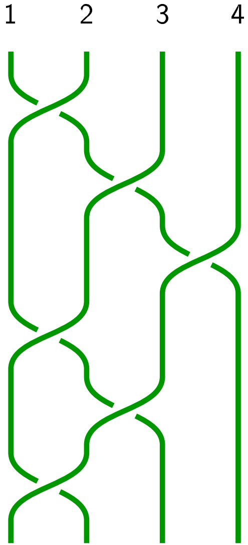
Far Commutativity: $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i + 1 < j$.



Triple relation: $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$.



The fundamental braid Δ



$\Delta = (\sigma_1\sigma_2\sigma_3)(\sigma_1\sigma_2)\sigma_1$

$$\begin{aligned} \mathbf{B}_N &= \langle \sigma_1, \ldots, \sigma_{N-1} \rangle \leq \mathbf{B} \\ \Delta &\in \mathbf{B}_N \\ \sigma_i \Delta &= \Delta \sigma_{N-i} \\ \Delta^2 &\in Z(\mathbf{B}_N) \\ \langle \Delta^2 \rangle &= Z(\mathbf{B}_N) \end{aligned}$$

Permutation braids and normal form

$a \leq b$: $\exists p \in \mathbf{B}_N{}^+, \; ap = b$.

$p \in S$: $1 \leq p \leq \Delta$.

Permutation braids: $P \cong^{\text{eff}} S_N$.
Canonical expression by transpositions $(i, i+1)$.

Adyan 1984–Thurston 1992–Elrifai–Morton 1994 Normal Form.

$$b = \Delta^{\inf(b)} p_1 p_2 \cdots p_\ell$$

$p_k \in S$ of maximal length, $k = 1, 2, \ldots, \ell$ (left-weighted).

Complexity: $|b|^2 N \log N$.

The Double Coset Problem and the Multiple CSP

$A, B \le G, g \in G, [A, B] = 1.$

BDH Problem. $(g^a, g^b) \mapsto g^{ab}$ $(a \in A, b \in B)$.

(A, B) Double Coset Problem. $agb \in AgB \mapsto \tilde{a} \in A, \tilde{b} \in B$, $agb = \tilde{a}g\tilde{b}$.

Shpilrain–Ushakov 2006. DCP $\ge$ BDH Problem.

Multiple CSP. $({g_1}^x, \ldots, {g_k}^x) \mapsto \tilde{x}$, $({g_1}^x, \ldots, {g_k}^x) = ({g_1}^{\tilde{x}}, \ldots, {g_k}^{\tilde{x}})$.

Parabolic Subgroup of $\mathbf{B}_N$: Conjugate of full subgroup on fewer strands.

E.g. $\mathbf{B}_{\{1,\ldots,\frac{N}{2}-1\}}, \mathbf{B}_{\{\frac{N}{2}+1,\ldots,N\}}$.

Garber–Kalka–Teicher–Ts 2012.
Multiple CSP $\ge$ DCP for parabolic subgroups.

Reduction of DCP to Multiple CP

(A,B) DCP. $agb \in AgB \mapsto \tilde{a} \in A, \tilde{b} \in B$, $agb = \tilde{a}g\tilde{b}$.

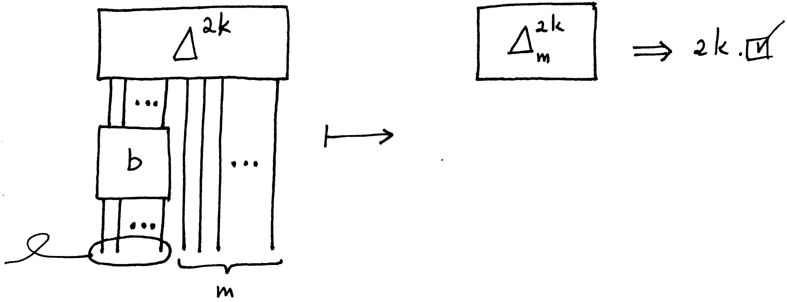
GKTTs. Multiple CSP $\geq$ DCP for parabolic subgroups $A, B \leq \mathbf{B}_N$:

1. Compute $C_{\mathbf{B}_N}(A) = \langle c_1, \ldots, c_k \rangle$, $C_{\mathbf{B}_N}(B) = \langle d_1, \ldots, d_m \rangle$.
   Using Paris 1997.
2. Solve

$$\begin{array}{rcl} {d_1}^b & = & d_1 \\ & \vdots & \\ {d_m}^b & = & d_m \end{array} \quad ; \quad \begin{array}{rcl} ({c_1}^g)^b & = & c_1^{\boxed{agb}} \\ & \vdots & \\ ({c_k}^g)^b & = & c_k^{\boxed{agb}} \end{array}$$

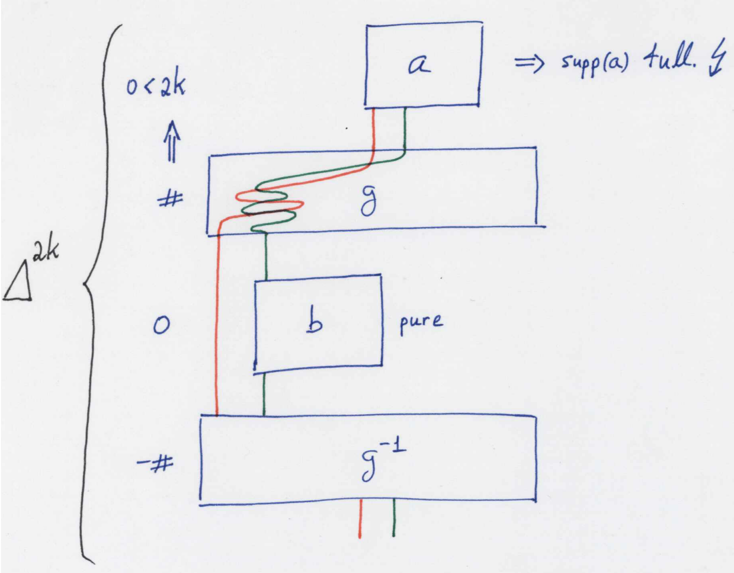
GKTTs. $B \leq \mathbf{B}_N$ parabolic $\Rightarrow C_{\mathbf{B}_N}(C_{\mathbf{B}_N}(B)) = \langle \Delta^2 \rangle \cdot B$.

Removing the Δ power efficiently



May leave one strand from b and one outside b.

No Δ powers



The Commutator Key Exchange Protocol

Anshel–Anshel–Goldfeld 1999.

Alice	**Public**	**Bob**
$v(x_1, \ldots, x_k) \in F_k$	$\langle a_1, \ldots, a_k \rangle \leq G$	$w(x_1, \ldots, x_k) \in F_k$
$a = v(a_1, \ldots, a_k)$	$\langle b_1, \ldots, b_k \rangle \leq G$	$b = w(b_1, \ldots, b_k)$

$$\xrightarrow{\quad {b_1}^{a}, \ldots, {b_k}^{a} \quad}$$

$$\xleftarrow{\quad {a_1}^{b}, \ldots, {a_k}^{b} \quad}$$

$K = a^{-1} v({a_1}^{b}, \ldots, {a_k}^{b})$ $\qquad$ $K = w({b_1}^{a}, \ldots, {b_k}^{a})^{-1} b$

$$a^{-1} v({a_1}^{b}, \ldots, {a_k}^{b}) = a^{-1} a^{b} = a^{-1} b^{-1} ab = (b^{a})^{-1} b = w({b_1}^{a}, \ldots, {b_k}^{a})^{-1} b$$

Additional reductions to the Multiple CSP

$a \in \langle a_1, \ldots, a_k \rangle, b \in \langle b_1, \ldots, b_k \rangle \leq G$.

Commutator KEP Problem.

$$({b_1}^a, \ldots, {b_k}^a, {a_1}^b, \ldots, {a_k}^b) \mapsto a^{-1}b^{-1}ab.$$

Shpilrain–Ushakov 2006. Multiple CSP $\geq$ Commutator KEP Problem when $C_G(a_1, \ldots, a_k) = Z(G)$ or $C_G(b_1, \ldots, b_k) = Z(G)$.

A.G. Myasnikov–Shpilrain–Ushakov 2006. $C_{\mathbf{B}_N}(\text{“}random\text{''}) = Z(\mathbf{B}_N)$.

Kalka–Liberman–Teicher 2009. Multiple CSP $\geq$ Dehornoy Shifted CSP.

Kalka–Liberman–Teicher 2010. Multiple CSP $\geq$ Garside-Subgroup CSP.

Part II

Solving the
Multiple Conjugacy Problem

Context: Garside groups

Generalizations of $\mathbf{B}_N$, by: Garside 1969 → Breiskorn–Saito, Deligne 1972 → Dehornoy–Paris 1999 → Dehornoy, Picantin, ...

Garside group:

1. left-multiplication invariant lattice order $(G, \leq, \wedge, \vee)$;
2. $\exists$ Garside element $\Delta \in G$:
   - 2.1 $S := \{g \in G \,:\, 1 \leq g \leq \Delta\}$ (simple elements) finite and generates G;
   - 2.2 Δ-conjugation preserves the monoid $G^+ := \{p \in G \,:\, 1 \leq p\}$;
   - 2.3 Weighted: $\exists$ homomorphism $(G^+, \cdot) \longrightarrow (\mathbb{N}, +)$.
   - 2.3′ General: Lengths of expressions by atoms are bounded.

The definition captures what is needed in existing proofs.

Finite invariants of conjugacy classes

Methodology. Efficiently computable:

1. $g \mapsto$ finite $I_g \subseteq g^G$;
2. $g \sim h \Rightarrow I_g = I_h$;
3. x with $g^x \in I_g$;
4. Compute I_g from any single element, by conjugations.

CSP Solution. Given $g \sim h$:

1. Conjugate g into I_g.
2. Conjugate h into $I_h = I_g$.
3. Build I_g by conjugations from g, until h's conjugate is found.

For Conjugacy Decision Problem: $I_h \cap I_g$ intersect?

Example: The free group

Think ring. Reduce cyclically (equivalently, cycle).

$$y^{-1}x^{-1}x^{-1}xyyxxy^{-1}xxy$$
$$x^{-1}x^{-1}xyyxxy^{-1}xx$$
$$x^{-1}xyyxxy^{-1}x$$
$$xyyxxy^{-1}$$

$$x^{-1}y^{-1}xxy^{-1}xyyyx$$
$$y^{-1}xxy^{-1}xyyy$$
$$xxy^{-1}xyy$$
$$xy^{-1}xyyx$$
$$y^{-1}xyyxx$$
$$xyyxxy^{-1}$$

$I_g :=$ all cyclic rotations of the cyclically reduced form of g
$=$ Cycle of the cycling orbit of g.

Inf, sup, and canonical length

Simple elements: $p \in [0,1] := \{p \in G \,:\, 1 \le p \le \Delta\}$.

$$\Delta^i \le \underbrace{\Delta^i p_1 \cdots p_\ell}_{\text{normal form of } b} \le \Delta^{i+\ell}.$$

Canonical length of b: ℓ.

$$\begin{aligned} \inf(b) &:= i \\ \sup(b) &:= i+\ell \\ b &\in [i, i+\ell] = [\inf(b), \sup(b)] \end{aligned}$$

$b \in [i, \infty)$: $i \le \inf(b)$.

Super Summit Sets

$\therefore \inf(b) \in \inf(b^{\mathbf{B}_N})$ is bounded from above.

$\overline{\inf}(b)$: Maximum of $\inf(b^{\mathbf{B}_N})$.

$\therefore b^{\mathbf{B}_N} \cap [\overline{\inf}(b), \infty)$ is finite nonempty.

Garside 1969 Summit Set: $SS(b) := b^{\mathbf{B}_N} \cap [\overline{\inf}(b), \infty)$.

Elrifai–Morton 1994.

$$\begin{aligned} \underline{\sup}(b) &:= \min(\sup(SS(b))) \\ SSS(b) &:= b^{\mathbf{B}_N} \cap [\overline{\inf}(b), \underline{\sup}(b)] \end{aligned}$$

Conjugating b into SSS(b)

In the free group, cycling brings g to the conjugacy invariant set.

Cycling in $\mathbf{B}_N$:

$$\Delta^i p_1 p_2 \cdots p_\ell = \overline{p_1} \Delta^i p_2 \cdots p_\ell \quad \longmapsto \quad \Delta^i p_2 \cdots p_\ell \overline{p_1},$$

and moving to normal form.

Conjugation by $\overline{p_1} = {p_1}^{\Delta^i}$.

i may only increase, ℓ may only decrease.

Elrifai–Morton 1994, Birman–Ko–Lee 2001. Cycling $|\Delta|$ times increases $\inf(b)$ (if not maximal).

DeCycling:

$$\Delta^i p_1 \cdots p_{\ell-1} p_\ell \quad \longmapsto \quad p_\ell \Delta^i p_1 \cdots p_{\ell-1} = \Delta^i \overline{p_\ell} p_1 \cdots p_{\ell-1}$$

+ normal form. Same results, for sup.

Computing SSS(b) from an element

Elrifai–Morton Convexity. SSS(b) is connected by conjugations by simple elements.

Franco–Gonzalez-Meneses 2003. $x, y \in S$,
$g, g^x, g^y \in \mathrm{SSS}(b) \Rightarrow g^{x \wedge y} \in \mathrm{SSS}(b)$.

$\therefore$ Enough to consider minimal simple elements above atoms of G^+.

Lee–Lee Algorithm

Lee–Lee 2002. For $\vec{g} = (g_1, \ldots, g_k) \in G^k$:

1. For $x \in G$, $\vec{g}^x = (g_1, \ldots, g_k)^x := (g_1^x, \ldots, g_k^x)$.
2. Multiple CSP. $\vec{g}^x \mapsto \tilde{x}$, $\vec{g}^x = \vec{g}^{\tilde{x}}$.
3. WLOG, $1 \leq x$.
4. If $\inf(g_i) < \overline{\inf}(g_i)$, then cycling according to g_i reduces $|x|$.

For a poset $\mathbb{P}$, extend $\leq$ to $\mathbb{P}^k$ coordinatewise:

$$(a_1, \ldots, a_k) \leq (b_1, \ldots, b_k) \iff a_1 \leq b_1, \ldots, a_k \leq b_k$$

For $\vec{g} = (g_1, \ldots, g_k) \in G^k$, $\inf(\vec{g}) := (\inf(g_1), \ldots, \inf(g_k))$.

$[\vec{i}, \infty) := \{\vec{g} \in G^k : \vec{i} \leq \inf(\vec{g})\}$.

$\therefore$ Algorithm to conjugate $\vec{g}^x$ into $[\inf(\vec{g}), \infty)$.

Garber–Kalka–Ts–Vinokur. Extends to (general) Garside groups.

Lee–Lee Solution to Multiple CSP in $\mathbf{B}_N$

Lee–Lee Convexity. $\vec{g}^G \cap [\vec{i}, \infty)$ is connected by conjugations by simple elements (permutation braids).

$\therefore$ Can construct $\vec{g}^G \cap [\inf(\vec{g}), \infty)$ in time $|\vec{g}^G \cap [\inf(\vec{g}), \infty)| \cdot |S|$.

Gonzalez–Meneses 2005. $x, y \in S$,
$g, g^x, g^y \in \vec{g}^G \cap [\vec{i}, \infty) \Rightarrow g^{x \wedge y} \in \vec{g}^G \cap [\vec{i}, \infty)$.

Reduces the factor $|S|$ to #atoms in G^+.

Garber–Kalka–Ts–Vinokur. Extends to weighted Garside groups.

$\vec{g}^G \cap [\inf(\vec{g}), \infty)$ is not a conjugacy invariant.

Experiments. $k = N$, $L = \lceil 2N \log N \rceil$, max size before aborting: $40,000$ (A = Aborted):

$N = 4$	A	1126	180	216	1082	11534	196	2774	608	136
$N = 8$	A	A	A	A	A	A	A	A	A	A

Application of the Lee–Lee solution

$a \in \langle a_1, \dots, a_k \rangle, b \in \langle b_1, \dots, b_k \rangle \leq G$.

Commutator KEP Problem.

$$(b_1{}^a, \dots, b_k{}^a, a_1{}^b, \dots, a_k{}^b) \mapsto a^{-1} b^{-1} ab.$$

A.G. Myasnikov–Shpilrain–Ushakov 2006:

1. For short generators, $\langle a_1, \dots, a_k \rangle = \mathbf{B}_N$ often.
2. By LBA, transform $(a_1, \dots, a_k)^b$ to $\vec{\sigma}^b := (\sigma_1, \dots, \sigma_{N-1})^b$.
3. $\vec{\sigma}^{\mathbf{B}_N} \cap [\,0, \infty\,) = \{\vec{x}, \vec{x}^\Delta\}$, so easy to solve.

Thus far no known efficient attack on Commutator KEP with intermediate length generators.

Our following algorithms will probably solve this problem.
(Not tested yet.)

Lexicographic SS

Garber–Kalka–Ts–Vinokur:

$\inf(\vec{g}) = (\inf(g_1), \ldots, \inf(g_k)) \leq (\overline{\inf}(g_1), \ldots, \overline{\inf}(g_k))$.

(Usually $(\overline{\inf}(g_1), \ldots, \overline{\inf}(g_k)) \notin \vec{g}^G$.)

$\therefore \exists$ lexicographic maximum, $\overline{\inf}(\vec{g})$, in $\inf(\vec{g}^G \cap [\inf(\vec{g}), \infty))$.

LexSS($\vec{g}$): $\vec{g}^G \cap [\overline{\inf}(\vec{g}), \infty)$.

Conjugating there: High jumper test using Lee–Lee.

Constructible by minimal simple elements. (Modifying Kalka–Liberman–Teicher 2010)

Experiments. Recall Lee–Lee set $> 40,000$ for $N = 8$.

$N = 8$	698	306	2	22	40	160	24	114	72	20
$N = 16$	A	A	A	A	A	A	A	A	A	A

Lexicographic SSS

Garber–Kalka–Ts–Vinokur:

$[\vec{i}, \vec{s}] := \{\vec{g} \in G^k \ : \ \vec{i} \le \inf(\vec{g}),\ \sup(\vec{g}) \le \vec{s}\}$.

$\underline{\sup}(\vec{g})$: Lexicographic minimum of

$$\sup(\mathrm{LexSS}(\vec{g})) = \sup(\vec{g}^G \cap [\overline{\inf}(\vec{g}), \infty)).$$

$\mathrm{LexSSS}(\vec{g})$: $\vec{g}^G \cap [\overline{\inf}(\vec{g}), \underline{\sup}(\vec{g})]$.

$\exists$ Algorithm for conjugating there + minimal simple elements for building it.

Experiments. Recall LexSS $> 40,000$ for $N = 16$.

$N = 16$	5720	24404	A	7192	32320	3696	A	A	A	A
$N = 32$	A	A	A	A	A	A	A	A	A	A

Concluding remarks and problems

Many natural problems reduce to the Multiple CSP.

So do some noncommutative-algebraic KEPs, in some situations.

We introduced the first computable, finite, multiple conjugacy invariants.

We solve Multiple CSP in arbitrary (not necessarily weighted) Garside groups.

In $\mathbf{B}_N$, can also use BKL representation, but improvement is small.

Can divide sizes of invariant sets by the order of $g \mapsto g^{\Delta}$.

We plan to solve the last remaining case of Commutator KEP (with the standard distribution) by combining our approach with A.G. Myasnikov–Shpilrain–Ushakov 2006.

Ultra Summit Sets for multiple conjugacy?